Amendment and Response
Applicant: Francisco Corella
Serial No.: 09/483,185
Filed: January 14, 2000
Docket No.: 10991054-1 (H300.116.101)
Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

REMARKS

This Response is responsive to the Non-Final Office Action mailed March 29, 2004. Claims 1-24 were rejected. Claims 1-24 remain pending in the application and are presented for reconsideration and allowance.

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected claims 1-3, 5, 6, 8, 10, 13, 14, 15, 17, and 18 under 35 U.S.C. § 103(a) as being unpatentable over Chapman U.S. Patent No. 6,058,484 in view of Hsu U.S. Patent No. 5,982,898.

The Examiner rejected claims 4 and 16 under 35 U.S.C. § 103(a) as being unpatentable over Chapman U.S. Patent No. 6,058,484 in view of Hsu U.S. Patent No. 5,982,898 in view of Assay U.S. Patent No. 5,903,882.

The Examiner rejected claims 7,9, 19, and 21 under 35 U.S.C. § 103(a) as being unpatentable over Chapman U.S. Patent No. 6,058,484 in view of Hsu U.S. Patent No. 5,982,898 in view of Howell U.S. Patent No. 5,276901.

The Examiner rejected claims 11 and 23 under 35 U.S.C. § 103(a) as being unpatentable over Chapman U.S. Patent No. 6,058,484 in view of Hsu U.S. Patent No. 5,982,898 in view of Maruyama U.S. Patent No. 6,393,563.

The Examiner rejected claims 12 and 24 under 35 U.S.C. § 103(a) as being unpatentable over Chapman U.S. Patent No. 6,058,484 in view of Hsu U.S. Patent No. 5,982,898 in view of Kausik U.S. Patent No. 6,263,446.

The Chapman et al. patent is directed to systems and methods for addressing problems associated with date settings discrepancies between client computer terminals and server computer terminals. The Chapman et al. patent teaches a scheme for selecting a certificate from a plurality of certificates, each of the plurality of certificates having a specific validity period. The selected certificate is selected because it has a desired validity period based on certain factors.

In the Office Action rejection of independent claims 1 and 13, the Examiner admits that the Chapman et al. patent does not disclose a short term public key certificate. Applicant respectfully submits that the Chapman et al. patent also does not teach or suggest any short

Amendment and Response
Applicant: Francisco Corella
Serial No.: 09/483,185
Filed: January 14, 2000
Docket No.: 10991054-1 (H300.116.101)
Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

term public key certificate, any directory for storing short term authorization information related to the user which is bound to the user's public key and long term identification information by the short term certificate, or any credentials server for issuing the short term certificate. All of these limitations are claimed in independent claim 1. Likewise, the Chapman et al. patent does not teach or suggest storing short term authorization information related to the user or issuing a short term certificate, as claimed in independent claim 13.

The Examiner further relies on the Hsu et al. patent as a basis for the § 103 obviousness rejection. The Hsu et al. patent is directed at solving problems with a certification approach, where the certificates are long-lived and there is a private key associated with each of the certificates. The Hsu et al. patent discloses that the certification overhead problems are ameliorated by separating the tasks of identity verification and certificate issuing, which allows a disassociating of the long-term binding between the subject and a public/private key pair. The Hsu et al. patent discloses a registration authority issuing a password to a subject after the subject submits proofs and information. The subject submits the password (or a hardware token) to a certification agent that determines whether the password is valid. If the password is valid, the certification agent constructs a certificate. The subject submits the certificate to a server that verifies the certificate and, if appropriate, concludes that communication with the subject can proceed.

The Hsu et al. patent teaches away from issuing a long-term public key identity certificate that binds a public key of the user to long-term identification information related to the user, as claimed in independent claims 1 and 13. The Hsu et al. patent teaches that there are problems with a certification approach, where the certificates are long-lived and there is a private key associated with each of the certificates. The Hsu et al. patent teaches that certification overhead problems are ameliorated by separating the tasks of identity verification and certificate issuing, which allows a disassociating of the long-term binding between the subject and a public/private key pair through the use of a password.

Applicant respectfully submits the Hsu et al. patent does not teach or suggest issuing a short-term public key credential certificate that binds the public key of the user to the long-term identification information related to the user from the long-term public key identity certificate and to the short-term authorization information related to the user, as claimed in independent claims 1 and 13, wherein the public key of the user is the public key of the user

Amendment and Response
Applicant: Francisco Corella
Serial No.: 09/483,185
Filed: January 14, 2000
Docket No.: 10991054-1 (H300.116.101)
Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

that is bound to the long-term identification information by the long-term public key identity certificate. By contrast, in the Hsu et al. patent, long-term identification information is not taken from a long-term public key identity certificate and public keys are not bound by a long-term public key identity certificate to long-term identification information. The Hsu et al. patent teaches that the certificate created based on the password differs in character from a typical long-lived certificate obtained from a certification authority. The Hsu et al. patent teaches that if the long-lived certificate is likened to a driver's license, then the certificate created based on the password can be likened to a subway token or a bus ticket. In the Hsu et al. patent, not even the password is included in the certificate created based on the password.

In view of the above, Applicant submits that all features of independent claim 1 and all features of independent claim 13 are not taught or suggested by the Chapman et al. and Hsu et al. patents alone or in combination. In addition, the Chapman et al. and Hsu et al. patents do not include any suggestion or motivation for combining features thereof to form the invention claimed in independent claims 1 and 13, and the Hsu et al. patent teaches away from combining features thereof to form the invention claimed in independent claims 1 and 13. The Chapman et al. patent concerns date setting discrepancies between client computer terminals and server computer terminals, and teaches selecting from a plurality of long-term certificates based on their validity dates. The Hsu et al. patent concerns ameliorating certification overhead problems by separating the tasks of identity verification and certificate issuing, which allows a disassociating of the long-term binding between the subject and a public/private key pair through the use of a password. Applicant respectfully submits there is no teaching, suggestion, or motivation to combine or modify the features of the Chapman et al. and Hsu et al. patents to achieve the public key authorization infrastructure of independent claim 1 or the method of independent claim 13 including issuing a long-term public key identity certificate that binds a public key of the user to long-term identification information related to the user and issuing a short-term public key credential certificate that binds the public key of the user to the long-term identification information related to the user contained in the long-term certificate and to short-term authorization information related to the user to achieve authorization of the user by an application program.

Amendment and Response
Applicant: Francisco Corella
Serial No.: 09/483,185
Filed: January 14, 2000
Docket No.: 10991054-1 (H300.116.101)
Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

Furthermore, as dependent claims 2-12 further define patentably distinct independent claim 1, and dependent claims 14-24 further define patentably distinct independent claim 13, these dependent claims are also believed to be allowable.

Therefore, Applicant respectfully requests reconsideration and withdrawal of the 35 U.S.C. § 103(a) rejections to claims 1-24, and allowance of all pending claims 1-24.

CONCLUSION

In view of the above, Applicant respectfully submits that pending claims 1-24 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and formal allowance of claims 1-24 is respectfully requested.

Amendment and Response
Applicant: Francisco Corella
Serial No.: 09/483,185
Filed: January 14, 2000
Docket No.: 10991054-1 (H300.116.101)
Title: AUTHORIZATION INFRASTRUCTURE BASED ON PUBLIC KEY CRYPTOGRAPHY

The Examiner is invited to contact the Applicant's representatives at the below-listed telephone numbers to facilitate prosecution of this application.

Any inquiry regarding this Response should be directed to either Patrick G. Billig at the below-listed telephone numbers or William J. Streeter at Telephone No. (970) 898-3886, Facsimile No. (970) 898-7247. In addition, all correspondence should continue to be directed to the following address:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400
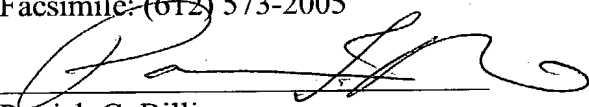
Respectfully submitted,

Francisco Corella

By his attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
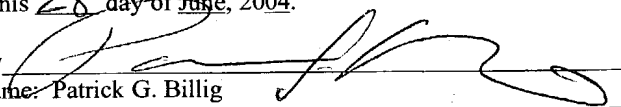Telephone: (612) 573-2003
Facsimile: (612) 573-2005

Date: June 28, 2004

PGB: kle

Patrick G. Billig
Reg. No. 38,080

BEST AVAILABLE COPY